Ejemplos de la configuración de resumen IPS

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Opciones del resumen](#)
[Resumen del evento](#)
[Configuración](#)
[Ataque de fuerza bruta de SSH - Firma 3653](#)
[Consulta SQL excesiva en los pedidos de HTTP - Firma 5474](#)
[Escáner interno o externo AD TCP/UDP - Firmas 13000 a 13008](#)
[Verificación](#)
[Troubleshooting](#)
[Información Relacionada](#)

Introducción

Este documento proporciona las explicaciones, las ventajas, y los ejemplos para la configuración del resumen en el (IPS) del Cisco Intrusion Prevention System.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad adaptante de Cisco (ASA) 5500 o módulos del (IPS) del Cisco Intrusion Prevention System 5500x
- IPS 4200, 4300, o dispositivos IPS de las 4500 Series
- Módulo NME-IPS
- Alertas de la firma IPS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Módulos ASA 5500 o 5500x IPS
- IPS 4200, dispositivos IPS de las 4300 o 4500 Series
- Módulo NME-IPS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Antecedentes

El resumen IPS proporciona los modos para agregar los eventos en una sola alerta, para poder disminuir el volumen de alertas enviadas por el sensor. Cada firma se crea con los valores por defecto que reflejan haber preferido, comportamiento normal. Sin embargo, cada firma tiene parámetros especiales que influencien cómo se manejan las alertas, así que el comportamiento predeterminado de las firmas se puede ajustar dentro de los apremios para cada tipo de motor.

Se procesan el resumen y las acciones del evento después de que el motor de la meta haya procesado los eventos componentes. Esto deja el sensor mirar para la actividad sospechosa sobre una serie de eventos.

La agregación básica proporciona dos modos:

- **Modo simple** - configura un número de umbral de golpes para una firma que deba ser resuelta antes de que se envíe la alerta.
- **Modo avanzado** - configura un número de umbral de golpes por segundo (cuenta del intervalo temporizado) para una firma que deba ser resuelta antes de que se envíe la alerta.

Opciones del resumen

- **fuego-todo** - Enciende una alerta cada vez que se acciona la firma. Si el umbral se fija para el resumen, las alertas se encienden para cada ejecución hasta que ocurra el resumen. Después de que el resumen comience, sólo una alerta para los fuegos de cada intervalo del resumen para cada conjunto del direccionamiento. Las alertas para otros conjuntos del direccionamiento se consideran todo o se resumen por separado. La firma invierte a fuego-**todo** modo después de un período de ningunas alertas para esa firma.
- **resumen** - Enciende una alerta la primera vez que se acciona una firma. Las alertas adicionales para esa firma se resumen para la duración del intervalo sumario. Solamente una alerta que cada intervalo sumario debe encender para cada conjunto del direccionamiento. Si se alcanza el umbral sumario global, la firma entra el modo del global-**resumen**.

- **global-resumen** - Enciende una alerta para cada intervalo sumario. Las firmas se pueden preconfigurar para el global-**resumen**.
- **fuego-una vez que** - Enciende una alerta para cada conjunto del direccionamiento. Este modo se puede actualizar al modo del global-**resumen**.

Resumen del evento

Un escenario frecuente es experimentar un período de línea de fondo que ajusta para identificar las firmas que alertan híperes. Hay a menudo varias firmas de bajo nivel y del nivel informativo que necesitan el resumen basado en la mezcla del tráfico. Revise estas firmas para determinar los umbrales apropiados.

> **Note**: Tenga cuidado siempre que usted reduzca la cantidad de alertas, especialmente las alertas de las firmas de la suma gravedad. Asegúrese de que la Seguridad no esté comprometida y de que las acciones apropiadas existen para cualquier firma se resuma que.

Configuración

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Ataque de fuerza bruta de SSH - Firma 3653

Las sesiones rápidas del Secure Shell (SSH), al activamente alertar, pueden llenar rápidamente el almacén del evento. Actualmente, se están negando las tentativas de la fuerza bruta de SSH.

Si usted necesita solamente las alertas cada cinco minutos, utilice la opción **sumaria** para la alerta-frecuencia con un resumen-intervalo de 300 segundos:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 3653 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode summarize
sensor(config-sig-sig-ale-sum)# summary-interval 300
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-sum)# show settings
alert-frequency
-----------------------------------------------
summary-mode
-----------------------------------------------
summarize
-----------------------------------------------
summary-interval: 300 default: 15
summary-key: Axxx <defaulted>
specify-global-summary-threshold
-----------------------------------------------
yes
```

```
-----------------------------------------------
global-summary-threshold: 240 <defaulted>
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Consulta SQL excesiva en los pedidos de HTTP - Firma 5474

Selecto-de la consulta SQL integrada en un pedido de HTTP es una de las firmas que alertan híperes mas comunes de un despliegue del borde.

Para ver la firma 5474 cada hora para un par del atacante/de la víctima, utilice fuego-**una vez que** opción para la alerta-frecuencia con un resumen-intervalo de 3600 segundos:

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 5474 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 3600
sensor(config-sig-sig-ale-fir-yes)# summary-interval 3600
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir)# show settings
fire-once
-----------------------------------------------
summary-key: Axxx default: Axxx
specify-global-summary-threshold
-----------------------------------------------
yes
-----------------------------------------------
global-summary-threshold: 3600 default: 240
summary-interval: 3600 default: 15
-----------------------------------------------
-----------------------------------------------
-----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Escáner interno o externo AD TCP/UDP - Firmas 13000 a 13008

En este ejemplo, los fuegos de la firma cuando detecta un (TCP) del Control Protocol del transporte/un escáner del User Datagram Protocol (UDP) que analice el conjunto de los IP Address de destino configurados como zona interna o externa. Si el administrador IPS expreso (IME) envía el valor por defecto, los eventos de la suma gravedad como notificaciones por correo electrónico, allí pudieron ser millares de correos electrónicos.

> **Note**: Aseegurese los fuegos no son un ataque del falso positivo. Cambie la configuración para que la Detección de anomalías “aprenden el modo” por 48 horas, después lo mueven

de nuevo a “detectan el modo” para resolver el problema.

Para reducir el número de correos electrónicos, utilice fuego-**una vez que** opción para la alerta-frecuencia, con un resumen-intervalo de 720 segundos o una vez de cada 12 minutos.

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 13000 0
sensor(config-sig-sig)# alert-frequency
sensor(config-sig-sig-ale)# summary-mode fire-once
sensor(config-sig-sig-ale-fir)# specify-global-summary-threshold yes
sensor(config-sig-sig-ale-fir-yes)# global-summary-threshold 720
sensor(config-sig-sig-ale-fir-yes)# summary-interval 720
sensor(config-sig-sig-ale-fir-yes)# exit
sensor(config-sig-sig-ale-fir-yes)# show settings
  fire-once
  ----------------------------------------------
     summary-key: Axxx <defaulted>
     specify-global-summary-threshold
     ----------------------------------------------
        yes
        ----------------------------------------------
           global-summary-threshold: 720 default: 240
           summary-interval: 720 default: 15
        ----------------------------------------------
     ----------------------------------------------
  ----------------------------------------------
sensor(config-sig-sig-ale-fir)# exit
sensor(config-sig-sig-ale)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Configurar la frecuencia alerta
- Guías de configuración IPS
- Soporte Técnico y Documentación - Cisco Systems